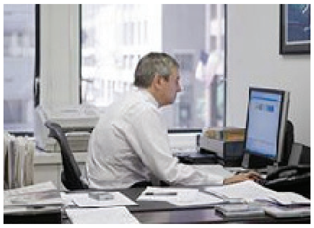
IronKey Trusted Access for Banking

Benefits:

- Protect commercial banking transactions
- Meet NACHA and FBI online banking guidelines
- Deliver rapid time to market
- Manage policy and updates remotely
- Reduce demands on customer service



"In the past six months, financial institutions, security companies, the media and law enforcement agencies are all reporting a significant increase in funds transfer fraud involving the exploitation of valid banking credentials belonging to small- and medium-sized businesses."

2009 NACHA and FBI Guidance to Financial Institutions

Keep Clients Safe from Financial Malware

Commercial banking is a target too large for criminals to ignore. Criminals are stealing hundreds of millions of dollars in schemes that attack banking clients' computers. With customizable malware frameworks such as Zeus readily available, a spectrum of malware ranging from unsophisticated copycats to highly targeted attacks are facing banking customers. Attacks frequently used by criminals include:

- Man-in-the-browser – A compromised computer allows criminals to tamper with transactions or actively initiate fraudulent transactions
- Man-in-the-middle – Hacked DNS or altered networking settings allow criminals to redirect users to forged websites for credentials theft
- Keylogging – Running in stealth, keyloggers can work in real-time to steal authentication credentials, even one-time passwords, for immediate use

To combat fraud, NACHA* and FBI developed guidelines for safe Web banking. These recommend that a dedicated, single-purpose computing environment be used only for online banking. To achieve this, Web browser, network connections, and even two-factor authentication, must be separate from the general purpose computing environment used for the Web, email, and work.

Tamper-proof Virtualization Provides a Safe Oasis for Banking

IronKey Trusted Access for Banking provides banking clients a secure connection isolated within a tamper-proof virtualized environment. Trusted Access for Banking is the only available solution that allows institutions to meet NACHA and FBI guidelines for safe online banking without added complexity and inconvenience.

A policy-controlled browser running inside a hardened, lightweight virtual machine is protected from host applications and malware. Keyboard input is encrypted from the host to virtual machine. This locks out malware from tampering with user activity and keyloggers from capturing passwords. All network and DNS activity run through a secure tunnel over IronKey's Trusted Network. Man-in-the-middle attacks or altered network settings cannot divert users to fraudulent sites.

Built on IronKey's portable USB security device, Trusted Access for Banking allows users to log on to their institution's authorized Web applications from multiple Windows computers. All applications, policies, and settings safely travel on tamper-proof USB storage. Optional automatic anti-virus scanning runs in the background to provide threat analytics. Integrated, onboard RSA SecurID provides users with a single strong authentication device. One-time password (OTP) entry is obfuscated to stop keyloggers and screen scrappers from stealing credentials.

Central Management and Automatic Updates Make Rollout Easy

Policy for Trusted Access for Banking is managed through the IronKey Enterprise Management Service. Deployments scale quickly without the need to procure data center space and setup hardware and software. Policies and users can be assembled into groups and managed independently from one another. Device usage and optional malware scan reports are available from the management console.

Administrator access can be delegated with differing access privileges and controls to allow customer service, auditing, and operations teams to perform their duties without compromising security or privacy. Support teams can assist users with password recovery and wipe devices if lost or stolen.

* NACHA – The Electronic Payments Association, formerly the National Automated Clearing House Association

Protect Commercial Banking Transactions & Meet NACHA and FBI Guidelines

Trusted Access for Banking allows clients to safely use commercial online banking from Windows computers. Malware and network attacks are locked out of the user's virtualized session.

- **Virtualized environment** – A hardened, lightweight operating system and Web browser run isolated from host applications and malware
- **Tamper-proof security** – Applications and settings can't be altered on the IronKey portable USB security device
- **Keylogging protection** – Input from the keyboard driver is encrypted to thwart keyloggers
- **Web address and IP access whitelisting** – Control which websites clients can access. To enforce location-based usage, access can be limited to specific IP range
- **Onboard RSA SecurID and protection option** – Onboard RSA SecurID allows users to carry a single authentication device. OTP is obfuscated to stop credential-stealing screen scrapers and keyloggers
- **Host anti-malware option** – Automatic McAfee anti-virus scanning identifies compromised systems

Manage Policies and Updates Remotely

Administrators can setup users, establish policies, and control client settings using the Enterprise Management Service operated in IronKey's secure data center.

- **Hosted management service** – The IronKey Enterprise Management Service runs 24x7 to provide administration and client policy updates
- **Automatic policy updates** – When a device is used, policy updates are requested and installed without user input
- **Remote wipe** – Disable devices if lost or stolen

Deliver Rapid Time to Market

The entire Trusted Access for Banking architecture is designed to enable institutions to quickly start rolling out a security solution to protect banking transactions.

- **Zero infrastructure** – No server hardware, software, or setup is required to go from evaluation to deployment
- **Portable USB security device** – Clients can move between multiple computers with automatic setup
- **Self-provisioned setup** – Devices are configured with policy and settings automatically during first-time use
- **Save confirmations** – Users can save transfer confirmations and other pages in PDF format to their desktop
- **Works with existing applications** – No server software or Web banking application modifications are required
- **Batch account import** – Bulk import new users
- **Branding –** Associate the security benefits with a brand by adding a logo to the user interface and optional physical branding on IronKey devices

Reduce Demands on Customer Service

Trusted Access for Banking is easy to use with automatic client setup. Management scales to support multiple levels of administrative access and reporting.

- **Delegated administration** – Provide multiple administrators and support staff with appropriate levels of policy control and access rights
- **Device usage reporting** – Automated device check-in provides detailed usage reports available from the Enterprise Management Service console

Technical Specifications

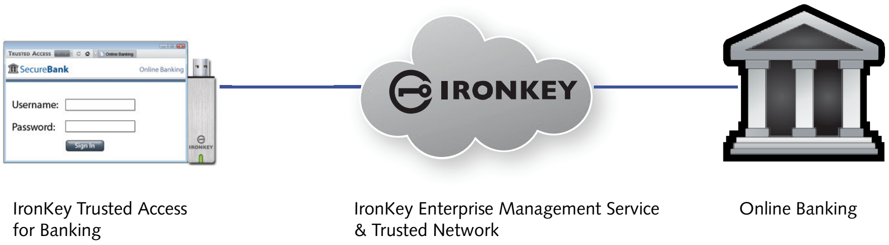
Trusted Access for Banking supports host systems running Windows 32-bit (XP, Vista, & 7) and 64-bit (Vista & 7) OS.

Using Trusted Access for Banking Overview

1) User inserts tamper-proof IronKey portable USB security device, Trusted Access for Banking launches automatically

2) Secure session initiated with Trusted Network, downloads policy updates configured with IronKey Enterprise Management Service

3) User connected to authorized bank site based on policy and authentication, protected from malware and network attacks


SecureBank
Online Banking
Username:
Password:
Sign In
IRONKEY
IronKey Trusted Access for Banking
IRONKEY
IronKey Enterprise Management Service & Trusted Network
Online Banking

www.ironkey.com
sales@ironkey.com
Toll-Free 866 645 9847

IronKey Headquarters
5150 El Camino Real, Suite C31
Los Altos, CA 94022 USA
T 650 492 4055   F 650 967 4650

European Office
6-9 The Square, Stockley Park
Uxbridge, Middlesex, UB11 1FW United Kingdom
T +44 (0) 203 1782 865   F +44 (0) 203 1782 866